AGENCY FOR INTERNATIONAL DEVELOPMENT

48 CFR Parts 739 and 752

0412-AA87

United States Agency for International Development Acquisition Regulation (AIDAR): Security and Information Technology Requirements.

AGENCY: U.S. Agency for International Development.

ACTION: Proposed rule.

SUMMARY: The U.S. Agency for International Development (USAID) seeks public comment on a proposed rule that would amend the USAID Acquisition Regulation (AIDAR) to incorporate a revised definition of information technology and other requirements relating to information security and information technology approvals. The Federal Information Technology Acquisition Reform Act requires improved management of the acquisition of Information technology resources. This proposed rule revising the AIDAR, if adopted, would provide increased oversight of contractor acquisition and use of information technology resources.

DATES: Comments must be received no later than [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER.]

ADDRESSES: Address all comments concerning this notice to Carol Ketrick, Bureau for Management, Office of Acquisition and Assistance, Policy Division (M/OAA/P), Room 867F, SA-44, Washington, D.C. 20523-2052. Submit comments, identified by title of the action and Regulatory Information Number (RIN) by any of the following methods:

1. Through the Federal eRulemaking Portal at http://www.regulations.gov by following the instructions for submitting comments.
2. By Mail addressed to: USAID, Bureau for Management, Office of Acquisition & Assistance, Policy Division, Room 867-F, SA-44, Washington, D.C. 20523-2052.

Comments on the information collection request under Section E, Paperwork Reduction Act must be submitted to both USAID and OMB/OIRA as follows:

USAID – Carol Ketrick at cketrick@usaid.gov.

OMB/OIRA – e-mail to oira_submission@omb.eop.gov, fax to (202) 395–6974, or mail to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street NW, Washington, DC 20503.

FOR FURTHER INFORMATION CONTACT: Carol Ketrick, Telephone: 202-567-4676 or e-mail: cketrick@usaid.gov

SUPPLEMENTARY INFORMATION:

A. Instructions:

All comments must be in writing and submitted through one of the methods specified in the Addresses section above. All submissions (and attachments) must include the title of the action and RIN for this rulemaking. Please include your name, title, organization, postal address, telephone number, and e-mail address in the text of the message. Please note that USAID recommends sending all comments to the Federal eRulemaking Portal because security screening precautions have slowed the delivery and dependability of surface mail to USAID/Washington.

All comments will be made available at http://www.regulations.gov for public review without change, including any personal information provided. We recommend that you do not submit information that you consider Confidential Business Information (CBI) or any information that is otherwise protected from disclosure by statute.

USAID will only address comments that explain why this proposed rule would be inappropriate, ineffective, or unacceptable without a change. Comments that are insubstantial or outside the scope of the rule may not be considered.

B. Background.

On September 5, 2014, the Office of Management and Budget (OMB) and the National Security Council (NSC) convened a President's Management Council, with one of the focus areas being improvement of cybersecurity in Federal acquisitions, in particular, accountability of contractors providing IT systems and services to the Federal government.

Accordingly, USAID is taking steps to address information security for information and information systems that support the operations and assets of the agency, including those managed by contractors. The new requirements will strengthen protections of Agency information systems/facilities.

Following the cybersecurity review directed by OMB "Follow-Up to President's Management Council Cybersecurity Meeting, September 5, 2014", which was completed by the agency Office of the Chief of Information Officer (CIO) in October 2014, a revised clause 752.204-72 Access to USAID facilities and USAID's Information Systems (now titled Homeland Security Presidential Directive-12 (HSPD-12) and Personal Identity Verification (PIV)), and new special contract requirements were developed and implemented on an interim basis under USAID Acquisition and Assistance Policy

Directive (AAPD) 16-02 SPECIAL CONTRACT REQUIREMENTS FOR INFORMATION TECHNOLOGY (IT) on May 3, 2016. The requirements in the AAPD were updated and reissued as AAPD 16-02 (Revised) on May 1, 2018. The policy published in the AAPD 16-02 (Revised) provides a new definition of information technology, and includes various requirements applicable to information and system security, as well as requirements for Electronic and Information Technology Accessibility, software licenses, and prior agency approval of IT purchases.

This AIDAR proposed rule, when finalized and effective, will establish the new definition, the revised AIDAR clause 752.204-72 Homeland Security Presidential Directive-12 (HSPD-12) and Personal Identity Verification (PIV), and AIDAR clauses based on some of the special contract requirements from the AAPD 16-02 (Revised). The remaining special contract requirements regarding information and system security in AAPD 16-02 (Revised) that are not included in this proposed rule will be assessed after finalization of the currently open FAR cases on Controlled Unclassified Information (CUI) and Breaches of Personally Identifiable Information (PII). In addition to the contract requirements originating from the AAPD 16-02 (Revised), a

proposed clause providing requirements for development and/or maintenance of third-party USAID-financed web sites is included in the rule.

Accordingly, USAID is proposing to amend the U.S. Agency for International Development (USAID) Acquisition Regulation (AIDAR) to revise various sections that will implement policy and procedures for contracts and orders for, or include a requirement for, information technology (IT) supplies, services and/or systems. These requirements will ensure that contractors comply with the current Agency IT policies. The requirements in this proposed rule would implement the requirements under the following authorities: the E-Government Act of 2002; Federal Information Technology Acquisition Reform ACT (FITARA)(Section 831 of the National Defense Authorization Act for Fiscal Year 2015, P.L. 113-291) and; Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) ("Section 508"); Privacy Act of 1974 (5 U.S.C. 552a - the Act); Federal Information Security Management Act (FISMA) of 2002 (FISMA, Public Law 107-347. 44 U.S.C. 3531-3536); National Institute of Standards and Technology (NIST) Special Publication 800-53 revision 4 or the current version; and Office of Management and Budget (OMB) Circular A-130.

USAID proposes to add AIDAR subpart 739, revise AIDAR 752.204-72, and include new clauses as follows:

• FAR subpart 739 provides the Agency definition of "information technology" as issued in AAPD 16-02 (Revised). As part of the AAPD 16-02 (Revised), a Class Deviation to FAR Part 2.101(b) definition of "information technology" was approved by the head of the contracting activity. This new definition broadens and clarifies the definition to include services such as cloud services; it is derived from the definition set forth in the Office of Management and Budget's (OMB's) guidance at OMB Memo M-15-14, Management Oversight of Federal Information Technology dated June 10, 2015. AIDAR 739.2 adds this definition, which also appears at 752.239-XX Use of Information Technology Approval and 752.239-XX Limitation on Use of Information Technology.

● AIDAR Clause 752.204-72 Access to USAID Facilities and USAID's Information Systems is being replaced in its entirety with a new title Homeland Security Presidential Directive-12 (HSPD-12) and Personal Identity Verification (PIV) and significant changes to reflect additional restrictions and reporting to better implement Homeland Security Presidential Directive-12 (HSPD-12) (August 27, 2004) and PIV procedures.

The revision improves requirements for contractor personnel provided access to agency facilities and information systems, as well as timely monitoring of such access when the employee's employment is terminated. The revised clause requires submission of staff reports listing employees that require access to USAID facilities or information systems, and also specifies the Agency's authority to suspend or terminate the access to any systems and/or facilities if an Information Security Incident or other electronic access violation, use, or misuse incident gives cause for such action.

- AIDAR 752.204-XX USAID-Financed Third-party Web Sites requires that Contractors adhere to certain requirements when developing, launching, and maintaining a third-party Web site funded by USAID for the purpose of meeting the project implementation goals. This applies to sites hosted on environments external to USAID boundaries and not directly controlled by USAID policies and staff. The clause requires adherence to Agency branding requirements and limits the contractor to collecting only the amount of information necessary to complete the specific business need as required by statute, regulation, or Executive Order.

- AIDAR 752.239-XX Limitation on Information Technology prohibits the acquisition of information technology under an award as defined in the clause unless prior approval is obtained from the contracting officer.

The clause ensures that only information technology approved by the Agency Chief Information officer (CIO) is acquired, pursuant to the Federal Information Technology Acquisition Reform ACT (FITARA)(Section 831 of the National Defense Authorization Act for Fiscal Year 2015, P.L. 113-291. All agency IT investment decisions, including software and IT equipment, must be made consistent with the agency's enterprise architecture. USAID must consider the total cost of ownership including the costs associated with risk issues, including security and privacy of data, and the costs of ensuring security of the IT system itself. This clause is consistent with the guidance promulgated by OMB in support of the Federal Information Technology Acquisition Reform Act (FITARA) and related information technology (IT) management practices in OMB Memo M-15-14 Management Oversight of Federal Information Technology.

- AIDAR 752.239-XX Software License addresses the need to ensure that acquired software is aligned with the agency's enterprise architecture; it will also enable the Agency to

consolidate licenses when appropriate in alignment with OMB Category Management Policy 16-1.

The clause clarifies that renewal of software licenses may only occur in accordance with the mutual agreement of the parties; or an option renewal clause allowing the Government to unilaterally exercise one or more options to extend the term of the award. Since renewal of a software license would require the obligation of funds by the Federal Government, renewal must not be automatic. Commercial off the shelf software solutions are offered to the public under standard agreements that may take a variety of forms, including license agreements, terms of service (TOS), terms of sale or purchase, and similar agreements. Customarily, these standard agreements contain terms and conditions that are appropriate when the purchaser is a private party but are inappropriate when the purchaser is the Federal Government.

- AIDAR 752.239-XX Information and Communication Technology (ICT) Accessibility requires contractors to implement Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) ("Section 508"). This clause applies to all development, procurement, maintenance, and information

communication technology for use by USAID and members of the U.S. public.

- AIDAR 752.239-XX Information Technology Approval requires that contractors acquire only the information technology specified in the contract, and specifies a process to request approval if the Contractor determines that acquisition of information technology is necessary to meet the Government's requirements under the award. The clause ensures that only information technology approved by the Agency Chief Information Officer (CIO) is acquired, pursuant to the Federal Information Technology Acquisition Reform ACT (FITARA)(Section 831 of the National Defense Authorization Act for Fiscal Year 2015, P.L. 113-291. All agency IT investment decisions, including software and IT equipment, must be made consistent with the agency's enterprise architecture. USAID must consider the total cost of ownership including the costs associated with risk issues, including security and privacy of data, and the costs of ensuring security of the IT system itself. This clause is consistent with the guidance promulgated by OMB in support of the Federal Information Technology Acquisition Reform Act (FITARA) and related information

technology (IT) management practices in OMB Memo M-15-14 Management Oversight of Federal Information Technology.

- AIDAR 752.239-XX Skills and Certification Requirements for Privacy and Security Staff requires that Contractor personnel performing the roles of Information System Security Officer and Information Security Specialists possess a Certified Information Systems Security Professional (CISSP) certification. All USAID contractors who have significant information security responsibilities as defined by OPM 5 CFR Part 930 must complete specialized IT security training.

Additionally, contractor personnel filling the role of Privacy Analysts must possess a Certified Information Privacy Professional (CIPP) credential with a CIPP/US to ensure that Privacy Analysts have the expertise required to implement U.S. government privacy laws, regulations and policies specific to government practice.

C. Regulatory Planning and Review.

This proposed rule has been determined to be "nonsignificant" under Executive Order 12866, Regulatory Planning and Review, dated September 30, 1993 and, therefore, is not subject to review.

This proposed rule is not a major rule under 5 U.S.C. §804.

D. Regulatory Flexibility Act. The proposed rule does not have a significant economic impact on a substantial number of small entities within the meaning of the Regulatory Flexibility Act, 5 U.S.C. §601, et seq. Therefore, an Initial Regulatory Flexibility Analysis has not been performed.

E. Paperwork Reduction Act

The Paperwork Reduction Act (44 U.S.C. chapter 35) applies. The proposed rule contains an information collection requirement. Accordingly, USAID has submitted a request to the Office of Management and Budget for approval of a new information collection requirement concerning "Access to USAID Facilities and USAID's Information Systems" and the monthly reports of employees requiring access.

"Access to USAID Facilities and USAID's Information Systems"

Public reporting burden for this collection of information is estimated to average initially eight hours immediately after contract award to develop the list of employee's requiring access, then 2 hours per month to update such a list, including the time for reviewing instructions,

gathering/maintaining the employee names, and forwarding the list to the agency for processing. The recordkeeping requirements are minor. While a contractor is required to identify and submit the list of its employees who require access, there is no requirement to collect this information in a particular format for submission to the agency.
The annual reporting burden is estimated as follows:

Total number of respondents and the amount of time estimated for an average respondent to respond: 138 contractors; eight hours for the initial report, 24 hours annually thereafter for submission of the monthly reports.

Total public burden (in hours) associated with the collection: 1104 hours initially, and 3,312 hours annually thereafter.

Total public burden (in cost) associated with the collection: Initial submission, $54,537, then $163,613 annually thereafter.

When submitting comments on these information collections, your comments should address one or more of the following four points:

(1) Evaluate whether the proposed collection of information is necessary for the proper performance of the

functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

(3) Ways to enhance the quality, utility, and clarity of the information to be collected; and

(4) Ways which USAID can minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses.

List of Subjects in 48 CFR parts 739 and 752:
Government procurement.

For the reasons discussed in the preamble, USAID amends 48 CFR parts 739 and 752 as set forth below:

1. Add part 739 to read as follows:

PART 739 --Acquisition of Information Technology

Sec

739.002 Definitions

739.003 [Reserved]

Authority: Sec. 621, Pub. L. 87-195, 75 Stat. 445, (22 U.S.C. 2381) as amended; E.O. 12163, Sept. 29, 1979, 44 FR 56673; and 3 CFR 1979 Comp., p. 435.

739.002 Definitions.

As used in this part—

Information Technology means

(1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

(2) Such services or equipment are "used by an agency" if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

(3) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

(4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

739.003 [Reserved].

PART 752 -- SOLICITATION PROVISIONS AND CONTRACT CLAUSES

2. The authority for part 752 continues to read as follows:

Authority: Sec. 621, Pub. L. 87-195, 75 Stat. 445, (22 U.S.C. 2381) as amended; E.O. 12163, Sept. 29, 1979, 44 FR 56673; and 3 CFR 1979 Comp., p. 435.

3. Amend section 752.204-72 by revising the section heading and the clause to read as follows:

752.204-72 Homeland Security Presidential Directive-12 (**HSPD-12) and Personal Identity Verification (PIV).**

*****

Homeland Security Presidential Directive-12 (**HSPD-12) and Personal Identity Verification (PIV)(DATE).**

(a) Individuals engaged in the performance of this award as employees, consultants, or volunteers of the contractor must comply with all applicable HSPD-12 and PIV procedures, as described below, and any subsequent USAID or Government-wide HSPD-12 and PIV procedures/policies.

(b) A U.S. citizen or resident alien engaged in the performance of this award as an employee, consultant, or volunteer of a U.S firm may obtain access to USAID facilities or logical access to USAID's information systems only when and to the extent necessary to carry out this award and in accordance with this clause. The contractor's employees, consultants, or volunteers who are not U.S. citizens or resident aliens as well as employees, consultants, or volunteers of non-U.S. firms, irrespective of their citizenship, will not be granted logical access to U.S. Government information technology systems (such as Phoenix, GLAAS, etc.) and must be escorted to use U.S. Government facilities (such as office space).

(c) (1) No later than five business days after award, the Contractor must provide to the Contracting Officer’s

Representative (COR) a complete list of employees that require access to USAID facilities or information systems.

(2) Before a contractor (or a contractor employee, consultant, or volunteer) or subcontractor at any tier may obtain a USAID ID (new or replacement) authorizing the individual routine access to USAID facilities in the United States, or logical access to USAID's information systems, the individual must provide two forms of identity source documents in original form to the Enrollment Office personnel when undergoing processing. One identity source document must be a valid Federal or State Government-issued picture ID. Contractors may contact the USAID Security Office to obtain the list of acceptable forms of documentation. Submission of these documents, to include documentation of security background investigations, is mandatory in order for the contractor to receive a PIV or PIV-Alternative (PIV-A)/Facilities Access Card (FAC) card and be granted access to any of USAID's information systems. All such individuals must physically present these two source documents for identity proofing at their enrollment.

(d) The Contractor must send a staffing report to the COR by the fifth day of each month. The report must contain the

listing of all staff members with access who were separated or hired under this contract in the past sixty (60) calendar days. This report must be submitted even if no separations or hiring occurred during the reporting period. Failure to submit the 'Contractor Staffing Change Report' each month may, at USAID's discretion, result in the suspension of all logical access to USAID information systems and/or facilities access associated with this contract. USAID will provide the contractor the format for this report.

(e) Contractor employees are strictly prohibited from sharing logical access to USAID information systems and Sensitive Information. USAID will disable accounts and revoke logical access to USAID IT systems if Contractor employees share accounts.

(f) USAID, at its discretion, may suspend or terminate the access to any systems and/or facilities when an Information Security Incident or electronic access violation, use, or misuse incident gives cause for such action. The suspension or termination may last until such time as USAID determines that the situation has been corrected or no longer exists.

(g) The Contractor must notify the COR and the USAID Service Desk at least five business days prior to the Contractor employee's removal from the contract. For unplanned terminations of Contractor employees, the Contractor must immediately notify the COR and the USAID Service Desk (CIO-HELPDESK@usaid.gov or (202)712-1234). The Contractor or its Facilities Security Officer must return USAID PIV/FAC cards and remote authentication tokens issued to Contractor employees to the COR prior to departure of the employee or upon completion or termination of the contract, whichever occurs first.

(h) The contractor is required to insert this clause (including this paragraph (h) in any subcontracts that require the subcontractor, subcontractor employee, or consultant to have routine physical access to USAID space or logical access to USAID's information systems.

(End of Clause)

4. Add section 752.204-XX to read as follows:

752.204-XX USAID-Financed Third-Party Web Sites.

Insert the following clause in USAID-funded solicitations and contracts that require development and/or maintenance of a third-party Web site to achieve project implementation goals.

USAID-Financed Third-Party Web Sites (DATE)

(a) Definitions: “Third-party Web Sites”

Web sites hosted on environments external to USAID boundaries and not directly controlled by USAID policies and staff, except through the terms and conditions of a contract. Third-party Web sites include project web sites.

(b) The contractor must adhere to the following requirements when developing, launching, and maintaining a third-party Web site funded by USAID for the purpose of meeting the project implementation goals:

(1) Prior to web site development, the Contractor must provide information as required in Section C-Statement of Work of the contract (including a copy of their Contractor’s privacy policy) to the Contracting Officer’s Representative (COR), for USAID's Bureau for Legislative and Public Affairs (LPA) evaluation and approval. The Contractor must notify the COR of the Web site URL as far in advance of the site's launch as possible and must not launch the web site until USAID's approval has been provided through the COR. The Contractor must provide the COR any changes to the Contractor’s privacy policy for the duration of the contract.

(2) The Contractor must collect only the amount of information necessary to complete the specific business need as required by statute, regulation, or Executive Order.

(3) The Contractor must comply with Agency branding and marking requirements comprised of the USAID logo and brandmark with the tagline “from the American people,” located on the USAID Web site at www.usaid.gov/branding, and USAID Graphics Standards manual at http://www.usaid.gov.

(4) The Web site must be marked on the index page of the site and every major entry point to the Web site with a disclaimer that states:

"The information provided on this Web site is not official U.S. Government information and does not represent the views or positions of the U.S. Agency for International Development or the U.S. Government."

(5) The Web site must provide persons with disabilities access to information that is comparable to the access available to others. As such, all site content must be compliant with the requirements of the Section 508 of the Rehabilitation Act, as amended (29 U.S.C. 794d) (“Section 508”) and other terms and conditions of the contract.

(6) The Contractor must identify and provide to the COR, in writing, the contact information for the Contractor's information security point of contact. The contractor is responsible for updating the contact information whenever there is a change in personnel assigned to this role.

(7) The Contractor must provide adequate protection from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted on the Web sites. To minimize security risks and ensure the integrity and availability of information, the Contractor must use sound: system/software management; engineering and development; and secure-coding practices consistent with USAID standards and information security best practices. Rigorous security safeguards, including but not limited to, virus protection; network intrusion detection and prevention programs; and vulnerability management systems must be implemented and critical security issues must be resolved as quickly as possible or within 30 calendar days. Contact the USAID Chief Information Security Officer (CISO) at ISSO@usaid.gov for specific standards and guidance.

(8) The Contractor must conduct periodic vulnerability scans, mitigate all security risks identified during such scans, and report subsequent remediation actions to CISO at

ISSO@usaid.gov and COR within 30 calendar days from the date vulnerabilities are identified. The report must include disclosure of the tools used to conduct the scans. Alternatively, the contractor may authorize USAID CISO at ISSO@usaid.gov to conduct periodic vulnerability scans via its Web-scanning program. The sole purpose of USAID scanning will be to minimize security risks. The Contractor will be responsible for taking the necessary remediation action and reporting to USAID as specified above.

(c) For general information, agency graphics, metadata, privacy policy, and Section 508 compliance requirements, refer to http://www.usaid.gov.

(End of Clause)

5. Add section 752.239-XX to read as follows:

752.239-XX Limitation on Acquisition of Information Technology.

Insert the following clause in all solicitations and contracts unless the special contract requirement Information Technology Approval is included.

Limitation on Acquisition of Information Technology (DATE)

(a) Definitions. As used in this contract:

Information Technology means

(1) Any services or equipment, or interconnected system(s)

or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

(2) such services or equipment are “used by an agency” if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

(3) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

(4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment.

(b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval of contracts that include information technology or information technology services.

(c) The Contractor must not acquire information technology as defined in this clause without the prior written approval by the contracting officer as specified in this clause.

(d) Request for Approval Requirements:

(1) If the Contractor determines that any information technology will be necessary to meet the Government's requirements or to facilitate activities in the Government's statement of work, the Contractor must request prior written approval from the Contracting Officer.

(2) As part of the request, the Contractor must provide the Contracting Officer a description and an estimate of the total cost of the information technology equipment, software, or services to be procured under this contract. The Contractor must simultaneously notify the Contracting Officer's Representative (COR) and the Office of the Chief Information Office at ITAuthorization@usaid.gov.

(e) The Contracting Officer will provide written approval to the Contractor through modification to the contract

expressly specifying the information technology equipment, software, or services approved for purchase by the COR and the Agency CIO. The Contracting Officer will include the applicable clauses and any special contract requirements in the modification.

(f) Except as specified in the contracting officer's written approval, the Government is not obligated to reimburse the Contractor for any costs incurred for information technology as defined in this clause. Such approval does not relieve the Contractor from the responsibility to maintain current compliance at all times--including through any updates or modifications to the information technology--with all terms and conditions of the contract, as well as relevant statutes and regulations.

(g) The Contractor must insert the substance of this clause, including this paragraph (g), in all subcontracts.

(End of Clause)

6. Add section 752.239-XX to read as follows:

752.239-XX Software License.

Insert the following clause in solicitations and contracts for new software licenses or to renew existing licenses, and in solicitations and contracts which may include a

requirement for new software licenses or renewal of existing licenses.

Software License Addendum (DATE)

(a) This clause incorporates certain terms and conditions relating to Federal procurement actions. The terms and conditions of this Addendum take precedence over the terms and conditions contained in any license agreement or other contract documents entered into between the parties.

(b) Governing Law: Federal procurement law and regulations, including the Contract Disputes Act, 41 U.S.C. Section 601 et. seq., and the Federal Acquisition Regulation (FAR), govern the agreement between the parties. Litigation arising out of this contract may be filed only in those fora that have jurisdiction over Federal procurement matters.

(c) Attorney's Fees: Attorney's fees are payable by the Federal government in any action arising under this contract only pursuant to the Equal Access in Justice Act, 5 U.S.C. Section 504.

(d) No Indemnification: The Federal government will not be liable for any claim for indemnification; such payments may violate the Anti-Deficiency Act, 31 U.S.C. Section 1341(a).

(e) Assignment: Payments may only be assigned in accordance with the Assignment of Claims Act, 31 U.S.C. Section 3727, and FAR Subpart 32.8, "Assignment of Claims."

(f) Patent and Copyright Infringement: Patent or copyright infringement suits brought against the United States as a party may only be defended by the U.S. Department of Justice (28 U.S.C. Section 516).

(g) Renewal of Support after Expiration of this Award: Service will not automatically renew after expiration of the initial term of award.

(h) Renewal may only occur in accord with (1) the mutual agreement of the parties; or (2) an option renewal clause allowing the Government to unilaterally exercise one or more options to extend the term of the award.

(End of Clause)

7. Add section 752.239-72 to read as follows:

752.239-72 Information and Communication Technology Accessibility.

Insert the following clause in solicitations and contracts that include acquisition of Information and Communication Technology (ICT) supplies and/or services for use by Federal employees or U.S. members of the public.

Information and Communication Technology Accessibility (DATE)

(a) Federal agencies are required by Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), to offer access to information and communication technology for disabled individuals within its employment, and for disabled members of the public seeking information and services. This access must be comparable to that which is offered to similar individuals who do not have disabilities. Standards for complying with this law are prescribed by the Architectural and Transportation Barriers Compliance Board ("The Access Board") in 36 CFR part 1194, which implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at http://www.access-board.gov/sec508/508standards.htm. The contractor must comply with any future updates of standards by the Access Board.

(b) Except as indicated elsewhere in the contract, all ICT procured through this contract must meet the applicable accessibility standards at 36 CFR part 1194 as follows:

(1) Section 1194.21 Software applications and operating systems

(2) 1194.22 Web-based intranet and Internet information and applications;

(3) Section 1194.23 Telecommunications products;

(4) Section 1194.24 Video and multimedia products;

(5) Section 1194.25 Self-contained, closed products;

(6) Section 1194.26 Desktop and portable computers;

(7) Section 1194.31 Functional performance criteria; and

(8) Section 1194.41 Information, documentation, and support.

(c) Deliverable(s) must incorporate these standards as well.

(d) The final work product must include documentation that the deliverable conforms with the Section 508 Standards promulgated by the US Access Board.

(End of Clause)

8. Add section 752.239-XX to read as follows:

752.239-XX Use of Information Technology Approval.

Insert the following clause in all USAID solicitations and contracts for Information Technology (IT) services or supplies or include a requirement for the contractor to provide IT services or supplies.

Use of Information Technology Notification (DATE)

(a) Definitions. As used in this contract:

Information Technology means

(1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

(2) Such services or equipment are “used by an agency” if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

(3) The term "information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

(4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (OMB M-15-14)

(b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval of contracts or interagency agreements for information technology or information technology services.

(c) The approved information technology and/or information technology services are specified in the Schedule of this contract. The Contractor must not acquire additional information technology without the prior written approval of the Contracting Officer as specified in this clause.

(d) Request for Approval Requirements:

(1) If the Contractor determines that any information technology in addition to that information technology specified in the Schedule will be necessary to meet the Government’s requirements or to facilitate activities in the Government’s statement of work, the Contractor must request prior written approval from the Contracting Officer.

(2) As part of the request, the Contractor must provide the Contracting Officer a description and an estimate of the total cost of the information technology equipment, software, or services to be procured under this contract. The Contractor must simultaneously notify the Contracting Officer's Representative (COR) and the Office of the Chief Information Officer at ITAuthorization@usaid.gov.

(e) The Contracting Officer will provide written approval to the Contractor expressly specifying the information technology equipment, software, or services approved for purchase by the COR and the Agency CIO. Additional clauses or special contract requirements may be applicable and will be incorporated by the Contracting Officer through a modification to the contract.

(f) Except as specified in the Contracting Officer's written approval, the Government is not obligated to reimburse the Contractor for costs incurred in excess of the information technology equipment, software or services specified in the Schedule. Such approval does not relieve the Contractor from the responsibility to maintain current compliance at all times--including through any updates or modifications to the information technology--with meeting

all terms and conditions of the contract, as well as relevant statutes and regulations.

(d) The Contractor must insert the substance of this clause, including this paragraph (g), in all subcontracts.

(End of Clause)

9. Add section 752.239-XX to read as follows:

752.239-XX Skills and Certification Requirements for Privacy and Security Staff.

Insert the following clause in solicitations and contracts for Information Technology (IT) services and in solicitations and contracts that include a component for IT services.

Skills and Certification Requirements for Privacy and Security Staff (DATE)

(a) Applicability: This clause applies to the Contractor, its subcontractors and personnel providing support under this contract and addresses the Privacy Act of 1974 (5 U.S.C. 552a - the Act) and Federal Information Security Management Act (FISMA) of 2002 (FISMA, Public Law 107-347. 44 U.S.C. 3531-3536).

(b) Contractor personnel filling the role of Information System Security Officer and Information Security Specialists must possess a Certified Information Systems

Security Professional (CISSP) certification at time of contract award and maintain their certification throughout the period of performance. This will fulfill the requirements for specialized training due to the continuing education requirements for the certification. Contractor personnel must provide proof of their certification status upon request.

(c) Contractor personnel filling the role of Privacy Analysts must possess a Certified Information Privacy Professional (CIPP) credential with a CIPP/USat the time of the contract award and must maintain the credential throughout the period of performance. This will fulfill the requirements for specialized training due to the continuing education requirements for the certification. Contractor personnel must provide proof of their certification status upon request.

(End of Clause)

Mark Walther,

Chief Acquisition Officer, Acting.

[FR Doc. 2019-04654 Filed: 3/20/2019 8:45 am; Publication Date: 3/21/2019]